UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA (Alexandria Division)

QUETEL CORPORATION, Plaintiff, v. HISHAM ABBAS, et al., Defendants.	Case No. 1:17-CV-00471 (AJT-JFA)

PLAINTIFF QUETEL CORPORATION'S MEMORANDUM IN SUPPORT OF ITS MOTION FOR SANCTIONS FOR DESTRUCTION OR SUPPRESSION OF DISCOVERABLE MATERIALS AND FOR FAILURE TO COMPLY WITH COURT ORDER

Plaintiff QueTel Corporation ("QueTel"), by counsel, respectfully submits this Memorandum in Support of its Motion for Sanctions for Destruction or Suppression of Discovery Materials and for Failure to Comply with Court Order ("Motion"), and states as follows:

INTRODUCTION

This case involves the theft of QueTel's proprietary software, known as TraQ Suite 6, by Defendant Hisham Abbas ("Abbas") and the knowing and willful infringement of QueTel's copyright for TraQ Suite 6 by Abbas, Defendant finalcover, LLC ("finalcover"), and Defendant Shorouk Mansour ("Mansour") (collectively, "Defendants"). QueTel alleges that Defendants misappropriated the TraQ Suite 6 source code, copied it and used it as the basis for their own competing software, known as CaseGuard. Defendants have denied QueTel's claims despite converging evidence that their position lacks merit.

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

As a copyright infringement and trade secrets case, a fundamental task in discovery is the comparison of the source code for the two competing software programs – not just in their current form, but through their history, dating back to the time of Defendants' theft of TraQ Suite 6, which occurred in or around April 2014, if not earlier. Defendants, however, have not produced any versions of their CaseGuard source code from in or around that time. Moreover, they have not produced what is known as a "source code control system," which, according to QueTel's expert in this matter, is the single most critical piece of evidence in a software misappropriation case. It contains all prior versions and changes to a software's source code, and was clearly in use before Defendants received a "cease and desist" letter on or about May 16, 2016. In essence, the source code control system, if produced, would permit QueTel to go back in time and perform a line-by-line, historical comparison of the two software programs' source code at critical points in time. Of note, such a comparison could prove infringement and trade secrets theft, without more, or potentially exonerate Defendants. Without it, the finder of fact is deprived of core evidence that would likely be central to important issues in this case (if not dispositive). Of grave concern, QueTel's expert has discovered evidence that Defendants have gone out of their way to obscure the fact that CaseGuard was copied from TraQ Suite 6 by refactoring CaseGuard's code.

Defendants have claimed that no source code control system exists, or has ever existed, for CaseGuard. They claim that Abbas did not use one. However, this claim has been debunked, albeit at great and unnecessary expense to QueTel. *First,* direct evidence of the use of a source code control system appears in a screen shot of CaseGuard's source code inadvertently shown to an employee of QueTel through social media in July 2014. *Second,* a forensic examination of Abbas's laptop (on which he claims to have developed CaseGuard), and standard industry

Cameron McEvoy PLLC
4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897

practices, confirm that a source code control system existed before Defendants received the above-referenced cease and desist letter. *Third*, Abbas has now admitted that in September 2016 he disposed of an older computer on which CaseGuard development occurred (and on which Abbas admits to having a source code control system), and replaced it with the device imaged and examined in this case. Yet despite considerable efforts to strip the new device of any evidence that a source code control system was used, Abbas was not successful. He should now be held to account.

In sum, Defendants have gone out of their way to destroy or conceal what can fairly be characterized as *the key piece of evidence* in this matter – the CaseGuard source code control system. They have done so after the Parties' disputes began, and after acknowledging a written demand to preserve evidence, with the intent to hinder QueTel's ability to prove its case. This is a grave violation of the discovery rules, and clear spoliation of evidence. Because Defendants' abuses of process strike at the heart the Federal Rules of Civil Procedure, and represent the opposite of everything that Fed. R. Civ. Pr. 1 enshrines as the hallmarks of a fair case, this Court should order an appropriate sanction under Fed. R. Civ. Pr. 37(b)(2)(A).

Specifically, given Defendants' extreme conduct, the Court should issue terminating sanctions, and enter default judgment against Defendants on its copyright and trade secret claims. Alternatively, QueTel requests that the Court (i) direct that it be taken as established in this case that Defendants misappropriated and copied TraQ Suite 6, and that TraQ Suite 6 are substantially similar, both objectively and subjectively, (ii) preclude Defendants from putting on any evidence that they did not copy Plaintiff's source code, or misappropriate Plaintiff's trade secrets, (iii) enter an Order requiring that certain jury instructions be given at the trial in this matter, or for other appropriate relief. In all cases, QueTel requests an award of fees and costs –

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

including all reasonable attorney's fees and expert fees – incurred as a result of Defendants' continued obfuscation.

FACTUAL AND PROCEDURAL BACKGROUND

I. Background Facts

QueTel has been a software development company since 1989. In 2009, it began developing a web-based asset tracking and evidence management software for law enforcement agencies, called TraQ Suite 6. In 2010, QueTel sold the first copies of this software. Since that time, QueTel has continued to develop TraQ Suite 6, adding approximately thirty optional features. These efforts have cost the company thousands of man hours and millions of dollars.

In June 2007, Abbas began working for QueTel and was directly involved with development of TraQ Suite 6. In June 2013, Abbas became the lead software developer at QueTel, a position he maintained until his resignation in April 2014. At the time of Abbas' resignation, the TraQ Suite 6 source code was over 200,000 lines long.

In January 2014, while still employed at QueTel, Defendant Abbas began identifying himself on social media as the CEO and co-founder of CaseGuard | finalcover (*see* Exhibit A). It is undisputed that finalcover's product (called CaseGuard) is also a web-based asset tracking and evidence management software for law enforcement agencies. Also in January 2014, finalcover, the entity which markets and sells CaseGuard, was formed. *See* Exh. B. finalcover is owned by Abbas and Mansour, who is Abbas' wife. At this time, is it not disputed that Abbas was still employed by QueTel at that time, and was its lead software developer, working on TraQ Suite 6.

Abbas resigned from QueTel in April 2014, but remained friendly with certain QueTel personnel, including Issa Salama ("Salama"), who took over as QueTel's lead software developer when Abbas resigned. On or about July 30, 2014, while engaged in a communication

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

on social media with Salama and others, Abbas showed the screen of his laptop to Salama for the purpose of sharing information about what to wear to a wedding. However, the screen also showed source code for CaseGuard on it (presumably inadvertently). Salama took a screenshot of the source code, which resembled TraQ Suite 6. A copy of the screenshot is attached hereto as Exhibit C.

On May 16, 2016, after it became known to QueTel that Defendants were actively engaging in competition with QueTel using CaseGuard (which was copied from TraQ Suite 6), QueTel's counsel sent a cease and desist letter to Defendants (Exhibit 3 to the Declaration of Monty G. Myers, attached as Exhibit D hereto). Included in this letter was a demand that Defendants produce a complete copy of the CaseGuard source code to QueTel for inspection, as well as a notice to "**preserve all potentially relevant evidence relating to the [development of the CaseGuard code]**." *Id.* (Emphasis in original).

On May 17, 2016 – just one day after the cease and desist letter was sent – Defendants responded, and, as is relevant to the instant motion, defended their actions by stating the screenshot of CaseGuard code that shows use of a source code control system (and striking similarities to TraQ Suite 6's code) "shows a very old version of Finalcover's code. Since this screenshot was taken in 2014, naming conventions and other assets have been fundamentally changed in [CaseGuard's] source code. The differences between Quetel and finalcover's code have thus only increased in the 2 years that Quetel has been sitting on this screenshot." *See* Exh. E, p. 2.

In late 2016, despite the above notice to preserve evidence in anticipation of litigation, Abbas disposed of the computer he used to develop CaseGuard. *See* Aug. 31, 2017 Letter from Defense Counsel (attached as Exhibit 2 to the Declaration of Monty Myers, Exhibit D hereto).

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

As discussed below, it has also become apparent through the course of discovery that Abbas – finalcover's principal – either disposed of or has withheld the production of a source code control system used with CaseGuard, the existence of which is now an undeniable fact.

II. Procedural History & Course of Discovery

On April 19, 2017, QueTel initiated this action by filing its Complaint (Docket No. 1). The Complaint alleges Copyright Infringement (Count I), Misappropriation of Trade Secrets, Va. Code §§ 59.1-336, *et seq.* (Count II), Violation of the Virginia Computer Crimes Act, Va. Code §§ 18.2-152.1, *et seq.* (Count III), Breach of Duty of Loyalty (Count IV, against Defendant Abbas only), Breach of Contract (Count V, against Defendant Abbas only), Tortious Interference with Contract and Business Expectancies (Count VI, against Defendant finalcover and Mansour), Conversion (Count VII), and Business Conspiracy, Va. Code §§ 18.2-499 and 500 (Count VIII). QueTel seeks damages, as well as injunctive relief (Docket No. 1).

On June 5, 2017, Defendants filed their Answer to the Complaint (Docket No. 9). On June 13, 2017, QueTel propounded upon Defendants its First Set of Requests for Production of Documents ("Document Requests") and its First Set of Interrogatories to each Defendant. Included in the Document Requests was a request for all versions of CaseGuard and the complete CaseGuard source code control system, which were to be produced in their complete native unmodified form, with the historical metadata preserved. *See, e.g.*, Exh. F, Request Nos. 5, 44 and Instructions.

On June 28, 2017, Defendants Abbas and Mansour (but not finalcover) each objected on the basis that it was "burdensome and overly broad and not reasonably calculated to lead to the discovery of admissible evidence." *See* Defendants Objections to Document Requests, at 22-23, 36. (attached hereto as Exhibit G). However, Defendants later withdrew their objections to

Cameron McEvoy PLLC
4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897

producing all versions of CaseGuard, its source code control system and the forensic image(s) of the devices used for CaseGuard's development. *See* Exh. H. However, Defendants represented – to their counsel and to QueTel's counsel – that there has only ever been one version of CaseGuard,[1] and that finalcover never had a source code control system. *See* Exhs. I, J.

On July 14, 2017, after unsuccessful, good faith efforts to resolve discovery disputes, QueTel filed its Motion to Compel Discovery, Overrule Defendants' Objections, and for Extension of QueTel's Expert Disclosure Deadline ("Motion to Compel") (Docket No. 19). On July 21, 2017, counsel for the parties appeared before this Court for argument. The Court ordered, *inter alia*, that Defendants must produce the CaseGuard source code control system, to the extent it still exists, as well as a forensic image of the device(s) used for the production/operation of CaseGuard. *See* Transcript of Hearing on Motion to Compel at 18-19 (attached hereto as Exhibit K). The Court ordered this production by July 28, 2017. *Id.*

Of note, the Court was persuaded that a source code control system for CaseGuard existed – at least as of July 30, 2014 (which was the date of the social media communication contained hereto at Exhibit C). *See* Exh. K at 19. The Court stated the following:

> THE COURT: All right. Well, I – given that the objections have been withdrawn to 5, 44 and 45 – and, you know, 44 asks for the source code control system, Source Safe, Git, or whatever application for this was being used, and the forensic image of the computer server used for the production/operation of the target system, those need to be produced.
>
> And I am going to give you until Friday of next week to do that, okay?
>
> MR. DeVRIES: Thank you, Your Honor.
>
> THE COURT: **But you need to understand, these have to be forensic images of those pieces of equipment and the complete source code system. So, to the extent that there is a source code system – and you need to make sure**

[1] This is entirely inconsistent with prior counsel's response to the cease and desist letter, which claimed multiple iterations of CaseGuard existed such that the 2016 version was far afield from its 2014 form, and from TraQ Suite 6.

Cameron McEvoy PLLC
4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897

> **your client understands what Mr. McEvoy has been presenting to the Court as far as what was resident on the computer at least at the point time [of the social media communication evidenced in the screenshot attached hereto as Exhibit C]**.
>
> …
>
> THE COURT: **So it was in 2014. I mean, that doesn't necessarily mean it's still there, but at one point in time it was there. So you'll need to deal with that issue.**

Id. at 18-19 (emphasis added).

On July 28, 2017, Defendants produced a forensic image of the computer server used for the production/operation of the target system. However, Defendants failed to produce the CaseGuard source code control system, and, to date, have not explained what happened to it. Moreover, the forensic image that was produced did not contain user files, as it turned out that Defendant Abbas had apparently not informed the forensic data collector that there was a second hard drive in the device at issue that also needed to be imaged. After this came to light, the second hard drive was ultimately imaged and produced on August 2, 2017.

QueTel's experts quickly determined that the forensic images on the drives were from a device that was first used in or about September 2016. This fact was communicated to Defendants' counsel on August 25, 2017, via email. *See* Exh. L. On August 31, 2017 counsel for Defendants responded by letter. *See* Exh. D, at Exh. 2. The August 31, 2017 letter contains representations from Abbas, as follows: "(1) while a source control system was installed on his 'old computer,' he did not use it to develop CaseGuard; (2) he copied his old computer's contents to a new computer but did not install a source control system on his new computer; (3) the forensic copy of his new computer did not contain a source control system because he did not install one; and (4) he does not have access to his old computer because he disposed of in [sic] late 2016." *Id*.

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

These new representations were provided to Monty G. Myers, QueTel's expert, and were incorporated into his analysis. Mr. Myers's conclusions and analysis are detailed in his expert report, which was timely produced to Defendants on September 5, 2017. Certain of those findings, which relate to the instant Motion, are set forth in his attached Declaration of Monty G. Myers (Exh. D hereto). Among the points made by Mr. Myers are the following:

Importance of a Source Code Control System

- "The source code control system is one of the most important and informative artifacts for cases such as this involving expert analysis related to allegations of theft and copying of software source code." Exh. D, ¶20.

- "A source code control system is a standard industry tool used to manage the entire life cycle of the source code created by software engineers. It is the official repository of record, contemporaneously capturing all changes to the source code over time. These systems serve as a detailed record of when software was created or added to a project as well as who made such changes and when they did so." *Id*., ¶20.

- "Such systems allow software engineers to look at the software at any relevant date in the history of its development. This ability to roll back in time to a previous version of the software is vital to a software developer when, inevitably, problems arise with a new release of the software or a version thereof. The source code control system also serves as a backup, and preserves the software's source code to prevent against deletion, corruption or other loss of the source code." *Id*., ¶21.

- "It is standard practice within the software development industry to use a source code control system. Indeed, it is essentially unheard of for commercial software to be managed without the use of a source code control system. In [Mr. Myers's] experience, this is true for both

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

small software development firms and the largest worldwide enterprises, irrespective of the number of developers." *Id*., ¶22.

- "Source code is the most important work product that software engineers create every day. Thus, it is important to maintain this complete history and to be able to revert and review historical versions when necessary. Importantly, source code control systems also contain various trial and/or research and development versions of the software that may not immediately make it to the current production software. It also contains removed or deprecated code. Finally, source code control systems are used for version and client/custom traceability management; when different users have different versions of the software, the source code control system helps ensure the development team is reviewing the appropriate version/product for each client or situation. Again, it is unthinkable that any reasonable developer would operate without using a source code control system." *Id*.

- "In [Mr. Myers's] experience as an expert in over eighty (80) matters, related to intellectual property, no single material has proven more important than source code control in clearly communicating critical elements of a product's development and the related project history behind the product. For purposes of a software source code comparison, like the one [Mr. Myers has] undertaken in this case, the source code control system used to develop the allegedly infringing code is often the single most critical piece of evidence. With access to the source code control system of the allegedly infringing code, the expert conducting the analysis of the code will generally be able to review the earlier versions of the allegedly infringing code and compare them with the applicable version of the code on which they allegedly infringe. Access to the earlier versions of the source code stored in a source code control system is particularly

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

important where, as is the case here, there is significant evidence of refactoring/obfuscation of the source code text of the allegedly infringing code." *Id.*, ¶23.

Evidence of Substantial Similarity

- "As a result of [Mr. Myers's] review of the TraQ Suite 6 and CaseGuard code [versions that Mr. Myers was actually able to access], I found that there are instances of fairly direct usage of the TraQ Suite 6 code in the CaseGuard code, as well as more indirect usage, where the original TraQ Suite 6 source code and structure was refactored somewhat but still reflective of the original source code." Exh. D, ¶15.

- "Many of the differences between TraQ Suite 6 and CaseGuard involve changes in class names, variable names and property names that could be easily done through a "Find and Replace" command in a code editing software package, with such change not impacting the functionality or performance of the software. Other differences involve changes in the code syntax while the overall logic of the software was kept substantially the same." *Id.*

- The lack of identical source code texts, in [Mr. Myers's] opinion, appears to be the result of substantial refactoring, if not obfuscation, on the part of Defendants. Many of the changes had no material functional relevance, but seem to have been made for the sole purpose of changing the visual expression of the code. In fact, in [Mr. Myers's] many years of experience in the industry and in providing expert services for copyright and trade secret matters, this case represents some of the most substantial refactoring/obfuscation I have observed." *Id.*

- "The structure of the CaseGuard software shares many common traits with the TraQ Suite 6 software. Not only are similar software classes used for similar purposes, but the names of the classes are often very close as well. Within the classes, property names, function names, and the logical structure of the classes in many cases are astonishingly close to one

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

another. Even when considering individual functions, the parameter names, parameter types, variable names, and variable types share obvious similarities. While there are syntax differences between the TraQ Suite 6 code and CaseGuard code, the logic used within the code is often very close and in some cases almost the same. [Mr. Myers has] found this pattern repeatedly while comparing the two code bases. The layout and logic of the equivalent CaseGuard file is strikingly similar to TraQ except for name changes[.]" *Id.*, ¶16(a).

- "For example, many of the classes, functions, properties, and variables have names that seem to follow a formula for renaming. Many of these names in the TraQ Suite 6 software have the same names in the CaseGuard software, but have the prefix "CG" or "Guard" added to the names as a prefix. In other examples, the prefix "TraQ" has been replaced with the prefix "CG" or "Guard" for class names, property names, function names, and variable names throughout the CaseGuard code." *Id.*, ¶16(b).

- "In general, it is clear to me that there has been a global replace of certain keywords in the CaseGuard software projects. In my opinion, these naming similarities cannot be attributed to mere coincidence, and it is clear to me that the CaseGuard code has been modified based on its origins as the TraQ Suite 6 software package." *Id.*, ¶16(c).

- "[Mr. Myers] further analyzed the nature of these similarities to determine if there are potentially other explanations for the unmistakable similarities in the code. An inspection of the code as well as searches for this code from public sources did not indicate any alternative source. Indeed, it is rather clear to persons skilled in the art that these similarities relate to areas where the programmer had creative choice and were not merely the product of the programmer basing his or her work on other public sources." *Id.*, ¶17.

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

- "Based upon the above-described direct comparative analysis of the TraQ Suite 6 and CaseGuard source code, it is my finding that TraQ Suite 6 and CaseGuard share multiple similarities suggesting and an unmistakable common source code lineage. The nature of these similarities indicates that this is not a coincidence." *Id*., ¶18.

- "However, what [Mr. Myers's] analysis could not accomplish, based on the materials that have been produced by the Defendants, is a direct, line-by-line comparison of the TraQ Suite 6 source code to prior versions of CaseGuard's source code, particularly the original or earliest versions of the CaseGuard code – the versions of the source code that would be most likely to contain evidence of literal copying of the TraQ Suite 6 source code. In [his] experience, these prior versions, and changes to them, are normally present and maintained by software developers on . . . a source code control system." *Id*., ¶19.

Evidence of Destruction or Concealment of Source Code Control System and Other Evidence

- "Defendants surprisingly initially claimed that they did not use such a system in developing CaseGuard. . . . This was highly unusual and is very unlikely in current software development practice, particularly for this type of software development project related to a commercial product." Exh. D, ¶24.

- "It is also inconsistent with evidence [Mr. Myers has] reviewed in preparing [his] expert report in this matter. First, [Mr. Myers] received and reviewed a screen shot of the source code for CaseGuard (attached to the Complaint as Exhibit C [and hereto as Exhibit C]). This screen shot shows Git bash client for Windows on the lower-left part of the screen. It also shows padlocks on the right. These padlocks indicate that version control is being used within the CaseGuard project that is being developed using Microsoft Visual Studio. **This, by itself, shows that Defendants were using a source code control system at the time of the social media**

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

discussion represented in the screenshot, which [was] on or about July 30, 2014." *Id*. at ¶25. (emphasis added).

- Additionally, Mr. Myers "reviewed the forensic images provided by Defendants pursuant to the Court's July 21, 2017 Order." *Id*., ¶27. Mr. Myers also reviewed an August 31, 2017 letter from Defendants' counsel, in which Abbas makes the following representations: "(1) while a source code control system was installed on his 'old computer,' he did not use it to develop CaseGuard; (2) he copied his old computer's contents to a new computer but did not install a source code control system on his new computer; (3) the forensic copy of his new computer did not contain a source code control system because he did not install one; and (4) he does not have access to his old computer because it was disposed of in late 2016." *Id*., ¶26.

- "[The forensic] images [produced by Defendants] flatly contradict Mr. Abbas' statements concerning the CaseGuard code, as relayed in the August 31, 2017 letter." *Id*., ¶27.

- "As an initial matter, the forensic images produced by Defendants were not consistent with [Mr. Myers's] understanding or expectations with respect to the production that Defendants were ordered to make. Given that there is evidence of CaseGuard code being written as far back as 2014, [Mr. Myers] expected to be provided with images of the computers that were being used to develop CaseGuard in the 2014 timeframe." *Id*., ¶28.

- "From the computer that the Defendants made available, two images were created. Analysis of the images indicates that computer's drives were not the same ones that were being used during development of CaseGuard in 2014. Forensic analysis shows that the file systems for the Operating System/Applications partition and one of the data drive's partitions were created in 2016, several months after a Cease and Desist letter was sent to the Defendants expressly informing them of their obligation to preserve evidence relevant to

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

QueTel's claims in this matter. Additionally, even though the other data partition shows a file system creation date of 2010, the creation dates of the user files on that partition match the same 2016 creation dates found on the other two partitions." *Id*., ¶29.

- [Mr. Myers's] forensic analysis also found clear evidence that one or more source code control systems were utilized by Defendant in conjunction with the CaseGuard product line. Forensic images show the use of the Subversion Source Code Control system with the CaseGuard Project. More specifically, [his] analysis revealed the existence of a folder - the ".svn folder" (shown in Exhibit 4 [to Mr. Myers' Declaration]) – which contains a revision of the CaseGuard software that was checked out from a server running the Subversion Version Control software – a source code control system. The files in this directory help the Subversion Version Control application recognize which source code files have been altered by the developer. The .svn Subversion folder was found in both forensic images that I received and analyzed. The dates of the files within this folder show a last written timestamp of January 5, 2015. Of note, [Mr. Myers's team] discovered this .svn folder only after performing a forensic analysis of the disk images created from the Defendant Abbas' computers. Remarkably, the materials previously produced in the case did not include these folders. Neither the zip file "Hisham Abbas - Lawyers Eyes Only.zip" contained on CD "CF-000001" nor the logical image of the \Development\CaseGuard folder "Finalcover_Development_CaseGuard_Folder.L01" contained these Subversion Version Control software related folders even though all evidence of source code control used for the CaseGuard project was requested to be produced. The fact that this source code control system had been clearly utilized for CaseGuard in the past was completely masked by Defendants' failure to reveal its existence. It was only through our detailed forensic review of the images that Defendants' produced in response to this Court's July 21, 2017 Order

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

that we were able to discover the above referenced evidence of Defendants' use of the Subversion Version Control software." *Id.*, ¶30.

- "Additionally, the forensic images show that Defendant Abbas used the Microsoft Visual Studio development environment. Visual Studio is an integrated development environment tool that is used by developers to create computer programs. It is the tool Defendant Abbas used for the development of the CaseGuard application. Visual Studio can be integrated with a source code control system. The Facebook screenshot from 2014 likewise shows Abbas's use of Visual Studio for his development of CaseGuard and such screenshot further shows the use of source code controls at that time as described above. **Indeed, [Mr. Myers's] independent testing confirmed that the only way that the Visual Studio pane displays the series of source code control related icons [as shown on the screenshot] is when Visual Studio is being utilized with a source code control system.**" *Id.*, ¶33.

- "A matter that is equally concerning is that the forensic analysis showed an intentional deletion of the version control software "Git for Windows" right before defendant was to produce his computer for forensic imaging. Git is a free and widely-used Version Control System. Analysis of Abbas' user registry file showed that the Git for Windows application was installed and had a shortcut place on the taskbar of the admin user (Defendant Abbas) on September 26, 2016, the date many other applications were installed and files copied to the computer. That application was then uninstalled on July 20, 2017, just six days before the forensic company arrived to take images of the Defendant's device." *Id.*, ¶34.

- "[Mr. Myers's] forensic analysis of the produced images identified the following information to support the fact that Defendants had intentionally manipulated evidence for the purpose of the litigation:

Cameron McEvoy PLLC
4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897

- The Operating System for the produced computer was installed on July 13, 2016, months after the Cease and Desist/Evidence Preservation letter was sent on May 16, 2016;
- Applications for the produced computer (e.g., Microsoft Visual Studio, SQL server etc.) were all installed on or after September 26, 2016;
- All user-created folders on the development partition (including the 'Development' folder) were created on or after September 26, 2016;
- The 'backups' folder on the backup partition which contains multiple backup versions of CaseGuard was created on September 26, 2016;
- Evidence of a mass copy of CaseGuard code related files into the 'Development' folder shortly after the 'Development' folder was created on the partition on September 26, 2016; and
- Thousands of CaseGuard related files were deleted from the Backups data partition on July 7, 2017." *Id.* ¶35.

- "In sum, it is [Mr. Myers's] opinion that, to a reasonable degree of professional certainty, Abbas is either suppressing or has destroyed his historical backups/copies (either in a source code control system or elsewhere), or he operated without any protection to secure his large body of development work. Based on [Mr. Myers's] experience, and [his] above-stated analysis-based opinion that Defendants used source code control with CaseGuard, it is further [his] opinion that it is far more likely that Defendant Abbas suppressed or destroyed the historical source code and source code control system than it is that he did not use reasonable backup protection such as source code control. **Indeed, the forensic evidence precludes a finding that Defendants never used a source code control system with CaseGuard."** *Id.*, ¶36. (emphasis added).

- In light of [Mr. Myers's] observations of significant refactoring/obfuscation, the number and nature of the material similarities between the two software systems, and Defendants apparent suppression or destruction of historical source code and source code control system, it is [his] opinion that the most likely reasonable explanation of such observations is that the TraQ

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

Suite 6 source code was originally copied by Defendants who then modified such source code over time." *Id*., ¶37.

- "Finally, it is [Mr. Myers's] opinion, that if [he] had been provided access to the source code control system for the CaseGuard product, such system would have documented the detailed historical changes to and evolution of the CaseGuard software – including the details of when and how Plaintiff's TraQ Suite 6 source code came to be introduced into Defendants' CaseGuard source code." *Id*., ¶38.

Defendants have been unmoved by QueTel's repeated requests for access to the CaseGuard source code control system and by this Court's July 21, 2017 Order. In response to a letter from QueTel's counsel dated September 8, 2017, Defendants have not even attempted to explain themselves, but have continued to insist that they do not have a source code control system for CaseGuard, and cannot produce it. In response to an inquiry regarding whether Defendants continue to insist that they never had one, Defendants have only continued to obfuscate. *See* Exh. M (Quetel's counsel's letter of September 8, 2017); Exh. D, at Exh. 6 (Sept. 14, 2017 letter from Defendants' counsel responding to Quetel's counsel's Sept. 8 letter). Notably, Defendants' latest response does not alter Mr. Myers' conclusions, and only enhances them. *See* Exh. D., ¶40.

It is apparent that Defendants are either concealing the source code control system or have destroyed it. QueTel is left with no other option but to request sanctions against Defendants, up to and including terminating sanctions.

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

ARGUMENT

I. QueTel Is Entitled to Sanctions Due To Defendants' Discovery Violations and Spoliation of Evidence.

Rule 37(b)(2)(A) provides that, in the event that "a party fails to obey an order to provide or permit discovery," the Court:

> may issue further just orders [including] . . . (i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims; (ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence; (iii) striking pleadings in whole or in part; . . . (v) dismissing the action or proceeding in whole or in part; (vi) rendering a default judgment against the disobedient party; or (vii) treating as contempt of court the failure to obey any order. Fed. R. Civ. P. 37(b)(2)(A).

Rule 37b grants the district court wide discretion to impose sanctions for a party's failure to comply with its discovery orders. *Mut. Fed. Sav. & Loan Ass'n v. Richards & Assocs., Inc.*, 872 F.2d 88, 92 (4th Cir. 1989).

In this case, there can be no doubt that QueTel is entitled to relief in the form of discovery sanctions given Defendants' conduct. *First*, QueTel requested copies of code and the source control system for that code that this Court then ordered to be produced. Defendants, despite overwhelming evidence to the contrary, continue to deny that they used a source control system for the CaseGuard softeware. Yet they have no answer or explanation for the migration and destruction of data that undeniably occurred in the period of July 2016 through September 2016, after the cease and desist letter had been received and answered. They also have no answer or explanation for why mass deletions of code occurred days and weeks before the Court-ordered forensic images were provided.

Second, the as explained by Mr. Myers and as the Court is well aware based on its own knowledge of past cases, the provenance of the source code is vital to a consideration of a full

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

and fair record, and to a just result. It would surely inculpate or exculpate, so there is no reason to suppress or destroy it unless it tends to show – likely clearly – that Defendants are liable for copyright infringement and trade secrets violations.

Third, QueTel would suffer considerable prejudice if sanctions are not awarded. Based on the screenshot attached hereto as Exhibit C, the May 17, 2017 letter from Defendants' original counsel admitting that there were multiple versions of the CaseGuard code, standard industry practice, and the findings of Mr. Myers, QueTel reasonably expected to prove its case without the relatively large forensic exercise necessitated by Defendants' denial that a source control system was used or ever existed, which has proven to be a false claim. Defendants have unfairly, and against the entire grain of the Federal Rules of Civil Procedure, suppressed or destroyed material evidence. The prejudice to QueTel from such suppression or destruction is manifest.

Fourth, QueTel is unable to cure Defendants' misconduct. Mr. Myers has stated that he has been deprived of the ability to conduct a line-by-line comparison that would yield the most precise analysis. This has meant that QueTel has had to spend unjustified sums to build a circumstantial case. While the evidence remains strong, that is beside the point. Plaintiff has had to pay more than it should for evidence of a lesser quality. That is grossly unfair.

Fifth, Defendants contumaciously insist that a source code control system does not exist, despite overwhelming evidence to the contrary, and core evidence has been made unavailable – intentionally – to the trier of fact. This means that both QueTel and the Court must spend more time on this matter than ever should have been the case had Defendants followed the rules.

Sixth, and finally, Defendants have provided no plausible explanation for their failure to produce the source code control system. In the face of clear evidence to the contrary, Defendant

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

Abbas has continued to represent that CaseGuard never used a source code control system. Defendants' position is untenable, as explained above. The only possibilities are that Defendants have either destroyed evidence or are concealing it. In either case, Defendants continue to be in violation of this Court's Order to produce the source code control system. For these reasons, sanctions are the only appropriate and just remedy for Defendants' failures to comply.

II. QueTel Is Entitled To Sanctions Due To Defendants' Spoliation Of Evidence.

Rule 37(e) states that, upon a party's failure to preserve electronically stored information that cannot be restored or replaced, the court may act in accordance with teh following:

> **(1)** upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> **(2)** only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> > **(A)** presume that the lost information was unfavorable to the party;
> >
> > **(B)** instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> **(C)** dismiss the action or enter a default judgment. Fed. R. Civ. P. 37(e).

Similarly, under the common law, to find that spoliation of evidence has occurred, a court must determine that there has been "willful destruction of evidence or failure to preserve potential evidence for another's use in pending or future litigation." *Trigon Ins. Co. v. U.S.*, 204 F.R.D. 277, 284 (E.D. Va. 2001). In "establish[ing] a claim of spoliation, a movant must show that the adverse party had a duty to preserve the allegedly spoiled [evidence] and that the [evidence was] intentionally destroyed." *Id.* at 285. "The degree of culpability and the prejudice suffered by the moving party will guide a Court in its formulation of remedial and punitive action." *Id.*

As discussed above, the evidence of intentional and prejudicial spoliation in this case is overwhelming. However, QueTel wishes to highlight certain pieces of evidence that go directly

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

to the issue of duty and intentionality. First, the timing of Abbas's disposal of his old computer shows that he had a duty to preserve it. The Fourth Circuit has observed that "the duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation." *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001). In this case, the duty to preserve CaseGuard's source code control system was firmly established by the transmission and receipt of the Cease and Desist Letter on May 16, 2016. That letter contained an express preservation notice that specifically referred to documents and other electronically stored information related to CaseGuard. *See* Exh. D, at Exh. 3. Defendants' prior counsel responded to the letter, referencing multiple iterations of the CaseGuard code. As an experienced software developer, it is inconceivable that Abbas would not have known the importance of a software control system to the case at hand. The duty to preserve is clear.

Intentionality is also beyond question in this case. "In the Fourth Circuit, any level of fault, whether it is bad faith, willfulness, gross negligence, or ordinary negligence, suffices to support a finding of spoliation." *E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc.*, 803 F. Supp. 2d 469, 497 (E.D. Va. 2011) (collecting cases on point). Here, there is evidence of not only negligence or even gross negligence, but willfulness and bad faith.

Despite receiving the Cease and Desist letter in May 2016 (which was addressed to Abbas personally and responded to the very next day), Abbas purchased his new, current computer in September 2016, and disposed of his old computer in "late 2016." *See*, Exh. D, at Exh. 2. Abbas has claimed that although he copied the "contents" of his old computer to his current device, that he did not install a source code control system on it. *Id*. He also continues to

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

insist that the source code control system was not used for CaseGuard, which, as Mr. Myers has found, simply is not true. *See id*., ¶36, & Exh. 2. Moreover, there is evidence of deletion of "Git for Windows" from the imaged device just days before the imaging ordered by this Court took place, and evidence of deletion of thousands of CaseGuard-related files on July 7, 2017, just two weeks prior. *See id*., ¶¶34, 35(f).

This all comes against the backdrop of Abbas's ever-changing story as to whether he has one or more versions of CaseGuard, and whether he ever had a source code control system for it. What Abbas would have the Court believe is that he developed CaseGuard entirely on his own, without preservation of backup versions to save against accidental deletion or corruption, or even to aid in the continued development of finalcover's flagship product. This is inconceivable, against the most basic tenets of commonsense, logic, and human nature, as well as being contrary to the evidence. The *only* remaining question is whether that system was destroyed or is being intentionally withheld, either of which justifies a finding of spoliation. If Abbas can be taken at his word at all (which is increasingly in doubt), then he does not have a source code control system to produce, which leads to only one conclusion: he intentionally failed to preserve it.

III. QueTel Is Entitled To Default Judgment And An Award Of Fees, Costs and Expenses Due To Defendants' Egregious Conduct.

a. Legal Standard for Terminating Sanctions.

The Court has discretion to choose among many options when fashioning a remedy for spoliation or discovery violations "for the purpose of leveling the evidentiary playing field and for the purpose of sanctioning the improper conduct." *See Vodusek v. Bayliner Marine Corp.*, 71 F.3d 148, 156 (4th Cir. 1995). In the spoliation context, the Fourth Circuit has stated that terminating sanctions, such as dismissal or default judgment, may be granted pursuant to the court's inherent authority to manage the judicial process, when either "(1) the spoliator's conduct

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

was so egregious as to amount to a forfeiture of his claim [or defense], or (2) that the effect of the spoliator's conduct was so prejudicial that it substantially denied the [non-offending party] the ability to [pursue] the claim." *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 593 (4th Cir. 2001). Bad faith is often a hallmark justifying dismissal or default, but, as the Fourth Circuit has noted, "even when conduct is less culpable, dismissal may be necessary if the prejudice to the [opposing party] is extraordinary, denying it the ability to adequately [make] its case." *Id.*[2]

A similar set of criteria have been applied when determining whether terminating sanctions are appropriate under Rule 37, as noted above. When determining whether a default judgment is an appropriate sanction, a court must apply a four-part test: "(1) whether the noncomplying party acted in bad faith; (2) the amount of prejudice his noncompliance caused his adversary, which necessarily includes an inquiry into the materiality of the evidence he failed to produce; (3) the need for deterrence of the particular sort of noncompliance; and (4) the effectiveness of less drastic sanctions." *Mut. Fed. Sav. & Loan Ass'n v. Richards & Assocs., Inc.*, 872 F.2d 88, 92 (4th Cir. 1989). "[T]he most flagrant case, where the party's noncompliance represents bad faith and callous disregard for the authority of the district court and the Rules, will result in the extreme sanction of dismissal or judgment by default." *Mut. Fed. Sav. & Loan Ass'n v. Richards & Assocs., Inc.*, 872 F.2d 88, 92 (4th Cir. 1989) (citing *Wilson v. Volkswagen of America, Inc.*, 561 F.2d 494, 503-06 (4th Cir. 1977).

b. <u>Defendants' Conduct Merits Entry Of Default Judgment On Counts I and II</u>.

While the above standards set a high bar, QueTel submits that Defendants' conduct is the type of flagrant and egregious behavior that justifies default judgment.

[2] Admittedly, dismissal or default "should be avoided if a lesser sanction will perform the necessary function." *See id.* at 590. However, as explained below, QueTel submits that no lesser sanction can perform all necessary functions in this instance, which include sanctioning and deterring improper conduct.

Cameron McEvoy PLLC
4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897

First, Defendants' actions demonstrate bad faith and callous disregard for this Court's authority and its Rules, with a high level of egregiousness and brazenness. "Destruction is willful when it is deliberate or intentional," whereas bad faith destruction occurs when a party engages in destruction "for the *purpose of depriving the adversary of evidence.*" *E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc.*, 803 F. Supp. 2d 469, 497 (E.D. Va. 2011) (internal citation omitted) (emphasis in original). Defendants are aware of the critical importance of the source code control system, yet have destroyed or concealed it throughout the course of discovery. They have done so despite receiving a Cease and Desist letter in May 2016, being served with this lawsuit in May 2017, receiving discovery requests seeking the source code control system specifically in June 2017, withdrawing objections to producing it on July 17, 2017, and being ordered to produce it by this Court on July 21, 2017. Defendants have taken and maintained the now-disproved position that they never had a source code control system for CaseGuard, despite overwhelming forensic evidence to the contrary, and despite the Court's own warning that it was clear the source code control system existed at one point, and that Defendants would have to deal with that issue. Defendants' steadfast denial of existing fact is, on the facts of this case, astounding and in bad faith.

Second, as noted above, Defendants have caused QueTel great prejudice. The source code control system is the *single most important piece of evidence* in this litigation. Expert analysis of CaseGuard's source code control system, which is essentially required in a case such as this,[3] would either prove or disprove the key issue in this case – the extent to which

[3] The issue of substantial similarity often turns on expert testimony, particularly in the software misappropriation context, where an analysis of code is necessary. *See, e.g.*, *Universal Furniture Int'l, Inc. v. Collezione Euorpa USA, Inc.*, 618 F.3d 417, 435 (4th Cir. 2010); *Computer Assocs. Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 713 (2d Cir. 1992) ("Thus, in deciding the limits to which expert opinion may be employed in ascertaining the substantial similarity of computer programs,

Cameron McEvoy PLLC
4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897

Defendants copied and/or used TraQ Suite 6's source code to develop CaseGuard. Where intentional, bad faith spoliation relates to *the crucial piece of evidence*, dismissal is appropriate. *See Silvestri*, 271 F.3d at 593.

Third, there is a need to deter this particular sort of noncompliance. Defendants' noncompliance has jeopardized QueTel's case. Ignoring Defendant's actions would "encourage other litigants to flirt with similar misconduct." *Mut. Fed. Sav. & Loan Ass'n*, 872 F.2d at 93. "To find otherwise would be to send the . . . message that the court may be pushed, ignored and defied to the outermost limits so long as the noncomplying party has even an inadequate fallback act ready in the wings should the final curtain be falling." *Id.* at 94. Defendants have ignored and defied the Court's ruling requiring the production of CasGuard's source code control system, and, more basically, the Federal Rules of Civil Procedure that require such production. They have done so by hiding behind provably untrue assertions, and, when presented with evidence of their falsity, continued to obfuscate, rather than simply admit to their concealment or destruction of the CaseGuard source code control system.

Fourth, no lesser sanction can be as effective as default judgment. Indeed, the "necessary function" is not performed when part of what is necessary is signaling to Defendants and to future litigants that such brazen disregard for Court procedures will not be tolerated. Moreover, remedies such as a jury instruction on the point, or creating evidentiary sanctions or striking parts of Defendants' answers, would be half-measures, as would permit Defendants to defend themselves on grounds other than attacking the copying of the code.

---

we cannot disregard the highly complicated and technical subject matter at the heart of these claims. Rather, we recognize the reality that computer programs are likely to be somewhat impenetrable by law observers – whether they be judges or juries.").

Cameron McEvoy PLLC
4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897

QueTel is aware of the Court's decision and analysis in the case of *BMG Rights Mgmt. (US) LLC, et al v. Cox Communications, Inc., et al.*, Civil Action No. 1:14-cv-1611, in which this Court considered a matter that also involved the spoliation of historical source code. In that case, Judge Anderson found that spoliation had occurred and recommended that the trial judge issue jury instructions regarding the spoliation and its effect on the litigation. *Id.*, Docket No. 447 at 6. Judge O'Grady, the trial judge, issued a jury instruction similar, but less forceful, than Judge Anderson's recommendation. *See BMG Rights Mgmt. (US) LLC v. Cox Communications, Inc.*, 199 F. Supp. 3d 958, 985 (E.D. Va. 2016).

With that decision in mind, QueTel does not make its request for terminating sanctions lightly. However, *BMG Rights Mgmt.* is distinguishable from the case at bar such that greater sanctions are appropriate and necessary here. First, in *BMG Rights Mgmt*., the non-disclosing party was not an actual party to the litigation but, instead, was a third-party agent of one of the plaintiffs. In this case, the spoliating party or parties are the named Defendants. Additionally, in *BMG Rights Mgmt.*, it was undisputed that no source code control system existed. It was this nonexistence of a source code control system combined with the offending party's continued alteration of the source code that led this Court to find that there had been intentional destruction of material information. However, here, the issue is much more grave. Defendants did not simply continue to edit their source code without properly preserving historical versions. Instead, they properly preserved historical versions of the source code and then either intentionally concealed or destroyed them.

Furthermore, in *BMG Rights Mgmt.*, this Court found that the offending party eventually produced various responsive "source code modules and scripts that were sufficient to show how" the relevant software system operated at the relevant time. Civil Action No. 1:14-cv-1611,

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

Docket No. 447, p. 2. However, in the case at bar, Defendants refuse to produce responsive source code modules and scripts that would show how CaseGuard source code appeared at the time most relevant to this litigation - its early development. The produced materials are largely dated in 2016, and prior code is missing.

Finally, in *BMG Rights Mgmt.*, this Court found that the moving party requested sanctions that would likely result in the dismissal of the plaintiffs' claims without considering other potential remedies available through the discovery process. *Id.* In contrast, the discovery process in this case holds no other potential remedies for QueTel. Deposing the source code developer is not a viable method to discover the material evidence at issue here, as it was in *BMG Rights Mgmt*. In this case, finalcover's lead source code developer is Abbas, who personally deleted a source code control system from his computer six days prior to its forensic imaging, and continues to lie about the very existence of a CaseGuard source code control system. Abbas' history eliminates any hope that his deposition would lead to the discovery of reliable, material evidence. Without the CaseGuard source code control system, QueTel has no ability to analyze historical versions CaseGuard source code to determine the level of copying of TraQ Suite 6 in the creation of CaseGuard – the fundamental task in this copyright litigation.

The facts of this case make it more analogous to the 2012 case if *Taylor v. Mitre Corp.*, No. 1:11-CV-1247, 2012 WL 5473573 (E.D. Va. Nov. 8, 2012). There, the plaintiff's action to "download and run a program whose express purpose is deletion of evidence *in direct response* to the Magistrate Judge's order that his computer be produced for inspection was to blatantly disregard his duties in the judicial system under which he sought relief. *Id.* at *2. Judge O'Grady found that the plaintiff "acted unilaterally, deliberately, and with full knowledge in deleting files from his computer," which justified terminating sanctions. *Id.* at *3.

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

Like the plaintiff in *Taylor*, Abbas, and, by extension, finalcover and Mansour, have intentionally deleted materials from a computer that would be highly relevant to the matter at hand, and, by their own words, have disposed of a prior device on which relevant materials were contained. They did so intentionally, and in response to the Order compelling the production of the device in question. Indeed, the latest evidence of spoliation -- deletion of the Git program from the device -- occurred on July 20, 2017, one day before this Court heard argument and ordered forensic imaging and production of the device in question, and three days after Defendants had withdrawn their objection to producing those images. This was less than two weeks after thousands of CaseGuard-related files were deleted from the imaged device. Though Abbas's actions were not in direct response to a Court order, the order on that particular point was a mere formality, given the withdrawal of Defendants' objections to producing the images. The only logical explanation for the deletions is that they were done in anticipation of the Court ordering forensic imaging. This is, of course, in addition to disposing of the prior computer, despite an obligation to preserve it, and the inexplicable failure to produce a source code control system for CaseGuard that is known to have existed, or to even explain what happened to it.

Defendants' obligation was to preserve and produce relevant evidence, including their source code control system for CaseGuard, as well as all prior versions of its source code. They have not done so, and have acted with total disregard for the Rules and Orders of this Court and the Federal Rules of Civil Procedure. Such brazen acts justify no less than terminating sanctions in the form of a default judgment.

CONCLUSION

For the foregoing reasons, and for those which will be further argued at the hearing on this Motion, QueTel respectfully requests that its Motion be granted, and that this Court enter an

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

Order of Default Judgment as to Counts I and II of the Complaint. In the alternative, QueTel requests that the Court exercise its discretion and fashion an appropriate remedy under common law and Rule 37 of the Federal Rules of Civil Procedure to address this problem, including but not limited to the following alternative remedies: (i) direct that it be taken as established in this case that Defendants misappropriated and copied TraQ Suite 6, and that TraQ Suite 6 are substantially similar, both objectively and subjectively, (ii) preclude Defendants from putting on any evidence that they did not copy Plaintiff's source code, or misappropriate Plaintiff's trade secrets, (iii) enter an Order requiring that certain jury instructions be given at the trial in this matter, or for other appropriate relief.. In all cases, QueTel requests that the Court order an award of fees and costs in its favor and against Defendants for all reasonable attorney's fees and expert expenses caused by Defendants' continued misconduct, as well as such other and further relief as justice may require.

DATE: September 22, 2017

Respectfully submitted,

QUETEL CORPORATION
By counsel

/s/ Timothy J. McEvoy

Timothy J. McEvoy, Esq.
VSB No. 33277
Patrick J. McDonald, Esq.
VSB No. 80678
CAMERON/MCEVOY PLLC
4100 Monument Corner Drive, Suite 420
Fairfax, Virginia 22030
703-273-8898 (Office)
703-273-8897 (Fax)
tmcevoy@cameronmcevoy.com
pmcdonald@cameronmcevoy.com
Counsel for Plaintiff QueTel Corporation

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC

CERTIFICATE OF SERVICE

I hereby certify that on this 22nd day of September, 2017, I filed the foregoing using the Court's CM/ECF system, which will send notice of electronic filing through the Court's electronic filing system to all counsel of record.

/s/ Timothy J. McEvoy
Timothy J. McEvoy, Esq. (VSB No. 33277)
Counsel for Plaintiff QueTel Corporation

4100 Monument Corner Drive, Suite 420, Fairfax, Virginia 22030
TEL 703.273.8898 FAX 703.273.8897
Cameron McEvoy PLLC